基于指示单光子源的非对称信道量子密钥分配

何业锋[1,2], 宋畅[2*], 李东琪[2], 康丹娜[2]

[1]西安邮电大学无线网络安全技术国家工程实验室, 陕西 西安 710121;

[2]西安邮电大学通信与信息工程学院, 陕西 西安 710121

摘要 针对传统的量子密钥分配协议未考虑非对称信道的问题,研究了基于指示单光子源的非对称信道的测量设备无关量子密钥分配协议的性能参数。主要分析了协议中的平均光子数、单边传输效率、密钥生成率与信道传输损耗之间的关系。比较了指示单光子源下,对称信道与非对称信道的测量设备无关量子密钥分配协议的性能优劣。仿真结果表明,随着信道传输损耗的增大,密钥生成率和安全传输距离逐渐减小,但非对称信道的性能仍优于对称信道的性能。

关键词 量子光学; 指示单光子源; 量子密钥分配; 测量设备无关; 非对称信道

中图分类号 TN918 **文献标识码** A **doi**: 10.3788/AOS201838.0327001

Asymmetric-Channel Quantum Key Distribution Based on Heralded Single-Photon Sources

He Yefeng[1,2], Song Chang[2], Li Dongqi[2], Kang Danna[2]

[1] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;

[2] *School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*

Abstract Aiming at the fact that the asymmetric channel is not considered in the traditional quantum key distribution (QKD) protocol, the performance parameters of measurement-device-independent QKD protocol for the asymmetric channel with heralded single-photon sources are investigated. The relationships between the mean-photon numbers, the unilateral transmission efficiency, the key generation rate and the channel transmission loss in the protocol are analyzed. The performances of measurement-device-independent QKD protocols with the heralded single-photon sources for symmetric and asymmetric channels are compared. The simulation results show that, as the channel transmission loss increases, the key generation rate and the safe transmission distance decrease gradually, but the performance for the asymmetric channel is still higher than that for the symmetric channel.

Key words quantum optics; heralded single-photon sources; quantum key distribution; measurement device independent; asymmetric channel

OCIS codes 270.3430; 270.5565; 270.5568; 190.4410

1 引 言

1984 年,Bennett 等[1]提出了第一个量子密钥分配(QKD)协议,即 BB84 协议,其基于量子力学和信息论的基本原理[2],具有无条件安全性,已成为国内外研究的热点[3-7]。然而,QKD 协议的无条件安全性只是理论上的,在实际应用中,使用设备的不完美性导致量子通信系统容易受到不同的攻击。例如,针对非理想光源的攻击有相位部分随机化攻击[8]和光子数分束(PNS)攻击等[9];针对非理想探测器的攻击有时移攻击[10]、探测器控制攻击[11-12]、致盲攻击等[13]。为了避免探测器的非完美性问题,

收稿日期: 2017-09-30; **收到修改稿日期**: 2017-10-26

基金项目: 国家重点研发计划(2017YFB0802000)、国家自然科学基金(61472472)、陕西省自然科学基础研究计划(2017JM6037)

作者简介: 何业锋(1978—),女,博士,副教授,主要从事网络安全和量子密码方面的研究。E-mail: yefenghe1978@163.com

* **通信联系人**。E-mail: SChang_402@163.com

2012 年，Lo 等[14]提出了一种测量设备无关的量子密钥分配(MDI-QKD)方案，该方案在不可信任的第三方进行 Bell 态测量(BSM)，避免了 QKD 系统中针对探测器侧信道的攻击。自该方案提出以来，其在理论和实际应用中均取得了一定的进展[15-19]。孙颖等[20]提出了一种基于纠缠光源和量子存储的 MDI-QKD 协议，分析了密钥生成率与安全传输距离、存储器量子态保持时间之间的关系。东晨等[21]通过使用奇相干光源，使 MDI-QKD 方案的安全密钥传输距离达到 200 km 以上，并且得到了奇相干光源的误码率上界和计数率下界。吴承峰等[22]通过引入单光子探测器的品质因子，得到了误码率与单光子探测器品质因子和分束器反射率之间的关系。在实际的 MDI-QKD 系统中，由于理想的单光子光源难以实现，一般使用弱相干态(WCS)光源，但是 WCS 光源中存在大量的真空脉冲和大比例的多光子脉冲，这导致传输效率受到限制(暗计数会导致远距离的比特翻转错误)，密钥生成率减小。Fasel 等[23-24]提出一种基于指示单光子源(HSPS)的 MDI-QKD 方案，该方案在发送端产生纠缠光子对，用其中一个光子指示另一个光子的到达时间，可增大接收脉冲中单光子的比率。文献[25-26]对基于 HSPS 的 MDI-QKD 协议进行了分析，得到了密钥生成率与安全传输距离之间的关系。Zhou 等[27]通过结合三强度诱骗态，提出了一种基于 HSPS 的 MDI-QKD 方案，得到了密钥生成率的下限和误码率的上限。在上述基于 HSPS 光源的 MDI-QKD 协议中，均假设通信双方到第三方的信道传输距离相同，而实际上，QKD 系统中存在信道传输距离不对称的情形，且这些参数对系统的性能有一定的影响。

本文分析了基于 HSPS 的非对称信道中，MDI-QKD 协议的密钥生成率与信道传输损耗间的关系，并研究了对称信道与非对称信道下距离比率对误码率及密钥生成率的影响，为 QKD 的应用提供了重要的理论参考。

2　基本原理

2.1　基于 HSPS 的 MDI-QKD 协议

基于 HSPS 的 MDI-QKD 系统模型如图 1 所示，其中 1H、2H、1V、2V 为四个单光子探测器的编号，PBS、BS、Pol-M 和 IM 分别代表偏振分束器、分束器、偏振调制器和强度调制器。把建立密钥的通信双方称为 Alice 和 Bob，第三方称为 Charlie，且 Charlie 可以是不受信任的。

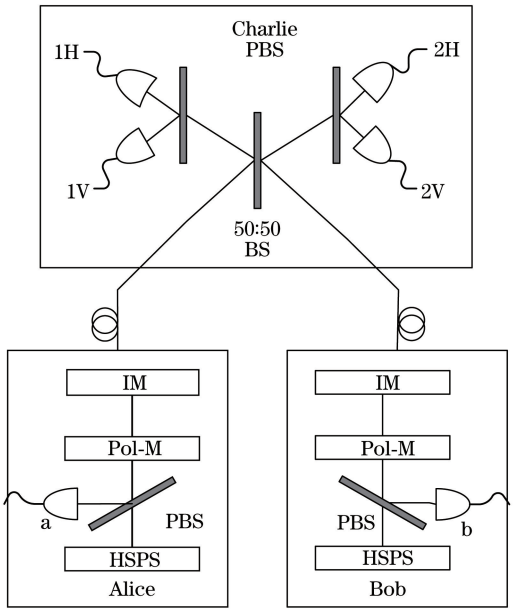

图 1　HSPS MDI-QKD 系统模型

Fig. 1　System model of HSPS MDI-QKD

HSPS 光源使用纠缠光子对中的一个光子来指示另一个光子的到达时间。由于纠缠光子之间具有同时性，因此可以精准地预测另一个光子的到达时间，再通过控制探测器的开关时间来增大接收脉冲中单光子的比率，进而增大 MDI-QKD 方案中的密钥生成率和传输距离。基于 HSPS 的 MDI-QKD 系统建立密钥的过程如下。

1) Alice 和 Bob 分别制备纠缠光子对，纠缠光子对通过偏振分束器，其中一个光子被分发给探测器，称为闲频光子。探测器每探测到一个闲频光子，就把另一个光子发送给 Charlie，称为信号光子。假定 Alice 和 Bob 使用的是阈值探测器，它只能判断是否有光子，r 表示探测结果，$r=0$ 表示探测器未被触发，$r=1$ 表示探测器被触发。输入一个 n 光子脉冲，η_1 表示探测成功的概率，η_0 表示探测失败的概率，则探测结果的概率 η_r 为

$$\eta_r=\left[(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n\right]^{(1-r)}\left[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n\right]^r,\tag{1}$$

式中 P_{d} 为探测器的暗计数率，η_{d} 为探测器的探测效率。假定仿真过程中所有探测器的参数是对应相同的。

2) 通过偏振调制器选取 X 基或者 Z 基进行偏振编码，X 基作为测试基用来估计信道参数，Z 基用来产生安全密钥。每个信号独立、随机地选择偏振状态。

3) 再经过强度调制器，将 Alice 和 Bob 的光脉

冲随机调制成三种强度：

$$\begin{cases}\{\mu_i\}, & i=0,1,2\\ \{v_j\}, & j=0,1,2\end{cases}, \tag{2}$$

式中 0,1,2 分别对应真空态、诱骗态和信号态，而且满足 $v_2>v_1>v_0=0$，$\mu_2>\mu_1>\mu_0=0$。

4) Charlie 对 Alice 和 Bob 发送过来的光脉冲作 BSM。当 D_{1H} 和 D_{1V} 同时响应，或 D_{2H} 和 D_{2V} 同时响应，表示投影到 Bell 态 $|\psi^+\rangle$。当 D_{1H} 和 D_{2V} 同时响应，或 D_{2H} 和 D_{1V} 同时响应，表示投影到 Bell 态 $|\psi^-\rangle$。其中 $|\psi^\pm\rangle=\frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle\pm|\leftrightarrow\rangle|\updownarrow\rangle)$，$|\leftrightarrow\rangle$ 表示水平偏振态，$|\updownarrow\rangle$ 表示竖直偏振态，以上四种响应情况均记为成功事件，其余为非成功事件[25]。等待所有的信号传输完毕，Charlie 公布所有测量结果。

5) Alice 和 Bob 根据 Charlie 公布的成功测量结果，对各自的比特进行翻转，翻转情况见表 1[15]，进而筛选密钥。

6) 对筛选后的结果进行纠错和保密加强处理，提高密钥的保密性，并最终获得安全密钥。

表 1　比特翻转操作[15]

Table 1　Bit-flipped operation[15]

Base	Project on $\|\psi^-\rangle$	Project on $\|\psi^+\rangle$
Z base	Bit-flip	Bit-flip
X base	Bit-flip	No change

2.2　公式推导

当探测器 a 和探测器 b 都响应之后，第三方再进行 BSM，即 Alice 和 Bob 只用激发探测器的光子脉冲来提取密钥，因此安全密钥的生成率[27]表示为

$$R\geqslant\frac{uv}{(1+u)^2(1+v)^2}Y_{11}^{z}[1-H(e_{11}^{x})]-Q_{uv}^{z,1,1}f(E_{uv}^{z,1,1})H(E_{uv}^{z,1,1}), \tag{3}$$

式中 $f(x)$ 为纠错效率函数；$H(x)=-x\ \mathrm{lb}(x)-(1-x)\mathrm{lb}(1-x)$ 为二进制香农熵函数，表示信源的平均不确定性；u 和 v 分别为 Alice 和 Bob 的脉冲强度。定义此时的增益和误码率分别为

$$Q_{uv}^{w,r_A,r_B}=\sum_{n,m=0}^{\infty}\frac{u^n v^m}{(1+u)^{n+1}(1+v)^{m+1}}\eta_{r_A}\eta_{r_B}Y_{nm}^{w}, \tag{4}$$

$$E_{uv}^{w,r_A,r_B}Q_{uv}^{w}=\sum_{n,m=0}^{\infty}\frac{u^n v^m}{(1+u)^{n+1}(1+v)^{m+1}}\eta_{r_A}\eta_{r_B}e_{nm}^{w}Y_{nm}^{w}, \tag{5}$$

式中 $w=x,z$ 表示 Alice 和 Bob 的编码方式采用 X 基或者 Z 基。η_{0A} 和 η_{0B} 分别为探测器 a、b 探测失败的概率；η_{1A} 和 η_{1B} 分别为探测器 a、b 探测成功的概率，η_{r_A} 和 η_{r_B} 分别为探测器 a、b 探测结果的概率。Y_{nm}^{w} 表示 Alice 发送 n 光子脉冲、Bob 发送 m 光子脉冲时获得成功 BSM 的概率，e_{nm}^{w} 为相对应的误码率，r_A 和 r_B 分别为 Alice 和 Bob 的探测器的探测结果，Q_{uv}^{11} 表示探测器 a 和 b 全都响应时的增益，$E_{uv}^{11}Q_{uv}^{11}$ 表示探测器 a 和 b 全都响应时的误码率。

进一步推出 Y_{11} 的下界值，从(4)式可以得到

$$\begin{aligned}(1+u)(1+v)Q_{uv}^{w,1,1}=&\sum_{n,m=0}^{\infty}\frac{u^n v^m}{(1+u)^n(1+v)^m}[1-(1-P_d)(1-\eta_d)^n]\times[1-(1-P_d)(1-\eta_d)^m]Y_{nm}^{w}=\\&\sum_{m=0}^{\infty}\frac{v^m P_d}{(1+v)^m}[1-(1-P_d)(1-\eta_d)^m]Y_{0m}^{w}+\frac{u}{1+u}\Big\{[1-(1-P_d)(1-\eta_d)]P_d Y_{10}+\\&\frac{v}{1+v}[1-(1-P_d)(1-\eta_d)]^2Y_{11}^{w}+\sum_{m=2}^{\infty}\frac{v^m}{(1+v)^m}[1-(1-P_d)(1-\eta_d)]\times\\&[1-(1-P_d)(1-\eta_d)^m]Y_{1m}^{w}\Big\}+\sum_{n=2}^{\infty}\frac{u^n}{(1+u)^n}[1-(1-P_d)(1-\eta_d)^n]\times\\&\Big\{P_d Y_{n0}^{w}+\frac{v}{1+v}[1-(1-P_d)(1-\eta_d)]Y_{n1}^{w}+\sum_{m=2}^{\infty}\frac{v^m}{(1+v)^m}[1-(1-P_d)(1-\eta_d)^m]Y_{nm}^{w}\Big\}=\\&(1+v)Q_{0v}^{1,1}+\frac{uv}{(1+u)(1+v)}\times[1-(1-P_d)(1-\eta_d)]^2Y_{11}+\\&(1+u)Q_{u0}^{1,1}-Q_{00}^{1,1}+h(u,v),\end{aligned} \tag{6}$$

式中

$$h(u,v)=\sum_{m=2}^{\infty}\frac{uv^m}{(1+u)(1+v)^m}[1-(1-P_{\mathrm{d}})\times(1-\eta_{\mathrm{d}})][1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^m]Y_{1m}+$$
$$\sum_{n=2}^{\infty}\frac{vu^n}{(1+v)(1+u)^n}[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})]\times[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n]Y_{n1}+$$
$$\sum_{n,m=2}^{\infty}\frac{u^nv^m}{(1+u)^n(1+v)^m}[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n]\times[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^m]Y_{nm}。\tag{7}$$

可以用 $Q_{u_1v_1}^{1,1}$ 和 $Q_{u_2v_2}^{1,1}$ 估计出 Y_{11} 的下界值。

$$(1+u_2)(1+v_2)Q_{u_2v_2}^{1,1}-(1+u_1)(1+v_1)Q_{u_1v_1}^{1,1}=$$
$$g_1+\left\{\frac{u_2v_2}{(1+u_2)(1+v_2)}[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})]^2-\frac{u_1v_1}{(1+u_1)(1+v_1)}[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})]^2\right\}Y_{11}+$$
$$\sum_{m=2}^{\infty}\left\{[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})][1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^m]\times\left[\frac{u_2v_2^m}{(1+u_2)(1+v_2)^m}-\frac{u_1v_1^m}{(1+u_1)(1+v_1)^m}\right]Y_{1m}\right\}+$$
$$\sum_{n=2}^{\infty}\left\{[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})][1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n]\times\left[\frac{v_2u_2^n}{(1+v_2)(1+u_2)^n}-\frac{v_1u_1^n}{(1+v_1)(1+u_1)^n}\right]Y_{n1}\right\}+$$
$$\sum_{m,n=2}^{\infty}\left\{[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^m][1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})^n]\times\left[\frac{v_2^mu_2^n}{(1+v_2)^m(1+u_2)^n}-\frac{v_1^mu_1^n}{(1+v_1)^m(1+u_1)^n}\right]Y_{nm}\right\}\geqslant$$
$$g_1+\left[\frac{u_2v_2\eta_{\mathrm{d}}^2}{(1+u_2)(1+v_2)}-\frac{u_1v_1\eta_{\mathrm{d}}^2}{(1+u_1)(1+v_1)}\right]\times Y_{11}+\kappa[h(u_2,v_1)+h(u_1,v_2)]=g_1+g_2+g_3-$$
$$\left[\frac{\kappa u_2v_1\eta_{\mathrm{d}}^2}{(1+u_2)(1+v_1)}+\frac{\kappa u_1v_2\eta_{\mathrm{d}}^2}{(1+u_1)(1+v_2)}-\frac{u_2v_2\eta_{\mathrm{d}}^2}{(1+u_2)(1+v_2)}+\frac{u_1v_1\eta_{\mathrm{d}}^2}{(1+u_1)(1+v_1)}\right]Y_{11},\tag{8}$$

当 $n,m\geqslant 2$ 时，有

$$\begin{cases}\dfrac{u_2v_2^m(1+u_1)(1+v_1)^m-u_1v_1^m(1+u_2)(1+v_2)^m}{u_2v_1^m(1+u_1)(1+v_2)^m+u_1v_2^m(1+u_2)(1+v_1)^m}\geqslant\\ \dfrac{u_2v_2^2(1+u_1)(1+v_1)^2-u_1v_1^2(1+u_2)(1+v_2)^2}{u_2v_1^2(1+u_1)(1+v_2)^2+u_1v_2^2(1+u_2)(1+v_1)^2}=a\geqslant 0,\\ \dfrac{u_2^nv_2(1+u_1)^n(1+v_1)-u_1^nv_1(1+u_2)^n(1+v_2)}{u_2^nv_1(1+u_1)^n(1+v_2)+u_1^nv_2(1+u_2)^n(1+v_1)}\geqslant\\ \dfrac{u_2v_2(1+u_1)^2(1+v_1)-u_1^2v_1(1+u_2)^2(1+v_2)}{u_2^2v_1(1+u_1)^2(1+v_2)+u_1^2v_2(1+u_2)^2(1+v_1)}=b\geqslant 0,\\ \dfrac{u_2^nv_2^m(1+u_1)^n(1+v_1)^m-u_1^nv_1^m(1+u_2)^n(1+v_2)^m}{u_2^nv_1^m(1+u_1)^n(1+v_2)^m+u_1^nv_2^m(1+u_2)^n(1+v_1)^m}\geqslant\\ \dfrac{u_2^2v_2^2(1+u_1)^2(1+v_1)^2-u_2^2v_1^2(1+u_2)^2(1+v_2)^2}{u_2^2v_1^2(1+u_1)^2(1+v_2)^2+u_2^2v_2^2(1+u_2)^2(1+v_1)^2}=c\geqslant 0。\end{cases}\tag{9}$$

令 $\kappa=\min\{a,b,c\}$，g_1，g_2，g_3 表示为

$$\begin{cases}g_1=(1+v_2)Q_{0v_2}^{1,1}-(1+v_1)Q_{0v_1}^{1,1}+(1+u_2)Q_{u_20}^{1,1}-(1+u_1)Q_{u_10}^{1,1}-Q_{00}^{1,1},\\ g_2=\kappa[(1+u_2)(1+v_1)Q_{u_2v_1}^{1,1}-(1+v_1)Q_{0v_1}^{1,1}-(1+u_2)Q_{u_20}^{1,1}+Q_{00}^{1,1}],\\ g_3=\kappa[(1+u_1)(1+v_2)Q_{u_1v_2}^{1,1}-(1+v_2)Q_{0v_2}^{1,1}-(1+u_1)Q_{u_10}^{1,1}+Q_{00}^{1,1}],\end{cases}\tag{10}$$

因此 Y_{11} 的下界值为

$$Y_{11}^{w}\geqslant\frac{g_1+g_2+g_3-(1+u_2)(1+v_2)Q_{u_2v_2}^{1,1}+(1+u_1)(1+v_1)Q_{u_1v_1}^{1,1}}{\dfrac{\kappa u_2v_1\eta_{\mathrm{d}}^2}{(1+u_2)(1+v_1)}+\dfrac{\kappa u_1v_2\eta_{\mathrm{d}}^2}{(1+u_1)(1+v_2)}-\dfrac{u_2v_2\eta_{\mathrm{d}}^2}{(1+u_2)(1+v_2)}+\dfrac{u_1v_1\eta_{\mathrm{d}}^2}{(1+u_1)(1+v_1)}}。\tag{11}$$

根据(5)式估计出 e_{11} 的最大值：

$$(1+u_1)(1+v_1)Q_{u_1v_1}^{1,1}E_{u_1v_1}^{1,1}=g_4+\frac{u_1v_1}{(1+u_1)(1+v_1)}[1-(1-P_{\mathrm{d}})(1-\eta_{\mathrm{d}})]^2\times Y_{11}e_{11}+h'(u_1,v_1),\tag{12}$$

式中

$$g_4=(1+v_1)Q_{0v_1}^{1,1}E_{0v_1}^{1,1}+(1+u_1)Q_{u_10}^{1,1}E_{u_10}^{1,1}-Q_{00}^{1,1}E_{00}^{1,1}, \tag{12a}$$

$$h'(u_1,v_1)=\sum_{m=2}^{\infty}\left\{\frac{u_1v_1^m}{(1+u_1)(1+v_1)^m}[1-(1-P_d)\times(1-\eta_d)][1-(1-P_d)(1-\eta_d)^m]Y_{1m}e_{1m}\right\}+\sum_{n=2}^{\infty}\left\{\frac{v_1u_1^n}{(1+v_1)(1+u_1)^n}[1-(1-P_d)(1-\eta_d)]\times[1-(1-P_d)(1-\eta_d)^n]Y_{n1}e_{n1}\right\}+\sum_{n,m=2}^{\infty}\left\{\frac{u_1^nv_1^m}{(1+u_1)^n(1+v_1)^m}[1-(1-P_d)(1-\eta_d)^n]\times[1-(1-P_d)(1-\eta_d)^m]Y_{nm}e_{nm}\right\}, \tag{12b}$$

可以得出

$$e_{11}^w\leqslant\frac{(1+u_1)^2(1+v_1)^2Q_{u_1v_1}^{1,1}E_{u_1v_1}^{1,1}-(1+u_1)(1+v_1)g_4^w}{u_1v_1\eta_d^2Y_{11}^w}。 \tag{13}$$

利用文献[6]可以推出 X 基下的增益和误码率分别为

$$Q_{u_iv_j}^{x,1,1}=2y_{ij}^2[1+2y_{ij}^2-4y_{ij}I_0(x_{ij})+I_0(2x_{ij})], \tag{14a}$$

$$E_{u_iv_j}^{x,1,1}Q_{u_iv_j}^{x,1,1}=e_0Q_{u_iv_j}^{x,1,1}-2(e_0-e_d)y_{ij}^2[I_0(2x_{ij})-1], \tag{14b}$$

式中 $I_0(x)\approx1+\frac{x^2}{4}$ 为修正贝塞尔函数，e_0 为偏正系数，e_d 为修正系数，而

$$Q_{u_iv_j}^{z,1,1}=Qc_{ij}+Qe_{ij}, \tag{15a}$$

$$E_{u_iv_j}^{z,1,1}Q_{u_iv_j}^{z,1,1}=e_dQc_{ij}+(1-e_d)Qe_{ij}, \tag{15b}$$

式中

$$Qc_{ij}=2(1-P_d)^2\exp(-u'_{ij}/2)\times[1-(1-P_d)\exp(-\eta_au_i/2)]\times[1-(1-P_d)\exp(-\eta_bv_j/2)], \tag{16a}$$

$$Qe_{ij}=[2P_d(1-P_d)^2\exp(-u'_{ij}/2)]\times[I_0(2x_{ij})-(1-P_d)\exp(-u'_{ij}/2)], \tag{16b}$$

参数分别为

$$u'_{ij}=\eta_au_i+\eta_bv_j, \tag{17a}$$

$$x_{ij}=\sqrt{\eta_au_i\eta_bv_j}/2, \tag{17b}$$

$$y_{ij}=(1-P_d)\exp(u'_{ij}/4), \tag{17c}$$

式中 u'_{ij} 为平均光子数，η_a，η_b 分别为 a、b 探测器的传输效率。

当信道为对称信道时，即 Alice 与 Charlie 之间的距离和 Bob 与 Charlie 之间的距离相等时（$L_{AC}=L_{BC}=L$），系统传输效率为信道传输效率 t 和探测效率 η_D 的乘积：

$$\eta=\eta_a=\eta_b=t\eta_D, \tag{18}$$

式中 $t=10^{-\alpha L/10}$。当信道为非对称信道时，即 $L_{AC}\neq L_{BC}$ 时，单边信道的传输效率分别为

$$t_{AC}=10^{-\alpha L_{AC}/10}, \tag{19a}$$

$$t_{BC}=10^{-\alpha L_{BC}/10}, \tag{19b}$$

式中 α 为信道传输损耗率。令此时非对称信道中的距离比为 $\sigma=L_{AC}/L_{BC}$（$0\leqslant\sigma\leqslant1$），即第三方的位置更靠近 Alice 一方。当 $\sigma=1$ 时，为对称信道，当 $0\leqslant\sigma<1$ 时为非对称信道。

由(18)式可以得到非对称信道的单边传输效率为

$$\begin{cases}\eta_a=\eta^{2\sigma/(\sigma+1)}\\ \eta_b=\eta^{2/(\sigma+1)}\end{cases}。 \tag{20}$$

因此，(17a)式中的平均光子数 u'_{ij} 可以表示为

$$u'_{ij}=\eta^{2\sigma/(\sigma+1)}u_i+\eta^{2/(\sigma+1)}v_j。 \tag{21}$$

通过改变第三方 Charlie 与 Alice 和 Bob 的距离影响单边传输效率，因此改变系统的传输效率，对密钥的生成率产生影响。

3　仿真结果

在仿真过程中，将(18)、(20)式代入到(17a)式，分别可以得到对称信道和非对称信道的系统平均光子数与信道传输损耗之间的关系，如图 2 所示，其中 f' 为纠错效率。将不同的 σ 值代入(20)式，可以得到不同 σ 值下，Alice 或者 Bob 的单边传输效率与信道传输损耗之间的关系，如图 3 所示。最后通过把(11)～(15)式代入(3)式中，得到最终的量子密钥生成率与信道传输损耗之间的关系，如图 4 所示。在仿真过程中，诱骗态和信号态的光子强度分别取 0.01 和 0.06，其他模拟参数值见表 2。

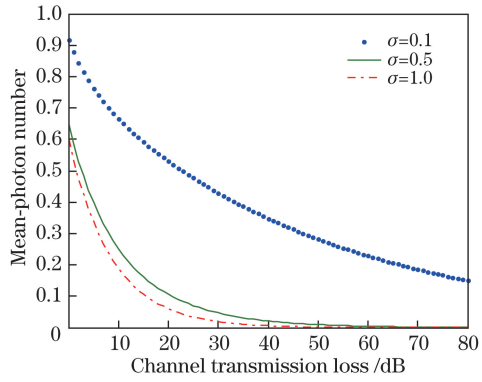

图 2　平均光子数与信道传输损耗间的关系

Fig. 2　Relationship between mean-photon number and channel transmission loss

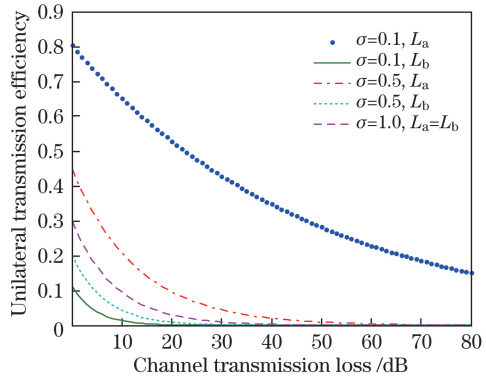

图 3　单边传输效率与信道传输损耗间的关系

Fig. 3　Relationship between unilateral transmission efficiency and channel transmission loss

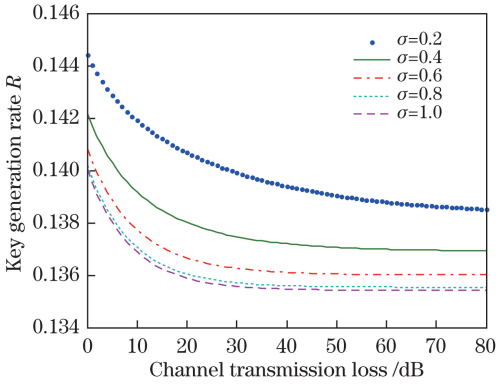

图 4　密钥生成率与信道传输损耗间的关系

Fig. 4　Relationship between key generation rate and channel transmission loss

表 2　数值模拟参数

Table 2　Numerical simulation parameters

Parameter	e_0	e_d /%	P_d	f'	η_d /pulse^{-1}
Value	0.5	1.5	3×10^{-6}	1.16	0.3

4　分析与讨论

如图 2 所示，随着信道传输损耗的增大，平均光子数呈现出递减的趋势。同时，平均光子数也和通信双方到第三方距离的比率有关，当信道的传输损耗相同时，随着距离比率的减小，平均光子数逐渐增大，即非对称信道具有比对称信道更大的平均光子数。这是因为当测量第三方逐渐向 Alice 靠近时，相当于传统 QKD 实验中的信号光强增大，发送脉冲中的多光子的比例比单光子的比例要大，所以最终的平均光子数增大。

如图 3 所示，随着信道传输损耗的增大，单边传输效率逐渐减小。信道对称时，单边传输效率的最大值为 0.3 dB。信道不对称即测量第三方向 Alice 靠近时，Alice 的输出脉冲在信道中的损耗减小，Alice 的单边传输效率逐渐增大。然而，Bob 的单边传输效率减小，这使得信道传输的不匹配度增大，单光子误码率增大。

如图 4 所示，随着信道传输损耗的增大，密钥生成率减小。当信道的传输损耗相同时，随着距离比的减小，Alice 的单边传输效率增大，输出脉冲在测量第三方成功进行 BSM 的概率增大，密钥生成率逐渐增大。即非对称信道的密钥生成率比对称信道的更大。

5　结　　论

研究了基于 HSPS 的非对称信道中，MDI-QKD 协议的密钥生成率与不同距离比之间的关系。在三强度诱骗态 MDI-QKD 协议下，比较了对称信道与非对称信道在不同距离比下的平均光子数、单边传输效率和密钥生成率与信道传输损耗之间的关系。根据仿真得到，随着距离比的减小，系统的密钥生成率增大，非对称信道的整体性能普遍优于对称信道的。在基于 HSPS 的 MDI-QKD 协议中，只用激发探测器的光子脉冲提取密钥，进行成功 BSM 的概率增大，使得系统的密钥生成率增大。因此，在实际应用中可以采用基于 HSPS 的非对称信道 QKD 来得到更大的密钥生成率。

参　考　文　献

[1] Bennett C H, Brassard G. An update on quantum cryptography[C]. Advances in Cryptology, 1984: 475-480.

[2] Zeng G H. Quantum cryptography[M]. Beijing: Science Press, 2006: 268-274.
曾贵华. 量子密码学[M]. 北京: 科学出版社, 2006: 268-274.

[3] Mizutani A, Tamaki K, Ikuta R, *et al*. Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol[J]. Physical Review Letters, 2012, 108(13): 130503.

[4] Du Y N, Xie W Z, Jin X, *et al*. Analysis on quantum bit error rate in measurement deviceindependent quantum key distribution using weak coherent states[J]. Acta Physica Sinica, 2015, 64(11): 110301.
杜亚男, 解文钟, 金璇, 等. 基于弱相干光源测量设备无关量子密钥分发系统的误码率分析[J]. 物理学报, 2015, 64(11): 110301.

[5] Sun S H, Gao M, Li C Y, *et al*. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[6] Ma X F, Razavi M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(5): 052305.

[7] Gong L H, Song H C, He C S, *et al*. A continuous variable quantum deterministic key distribution based on two-mode squeezed states[J]. Physica Scripta, 2014, 89(3): 035101.

[8] Sun S H, Liang L M. Experimental demonstration of an active phase randomization and monitor module for quantum key distribution[J]. Applied Physics Letters, 2012, 101(7): 071107.

[9] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols[J]. Journal of Modern Optics, 2011, 58(8): 680-685.

[10] Zhao Y, Fung C H F, Qi B, *et al*. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 2008, 78(4): 042333.

[11] Thomas O, Yuan Z L, Dynes J F, *et al*. Efficient photon number detection with silicon avalanche photodiodes[J]. Applied Physics Letters, 2010, 97(3): 031102.

[12] Gerhardt I, Liu Q, Lamaslinares A, *et al*. Full-field implementation of a perfect eavesdropper on a quantum cryptography system[J]. Nature Communications, 2011, 2(1): 349.

[13] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols[J]. Quantum Information & Computation, 2007, 8(6): 622-635.

[14] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13): 130503.

[15] Yu Z W, Zhou Y H, Wang X B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method[J]. Physical Review A, 2015, 91(3): 032318.

[16] da Silva T F, Vitoreti D, Xavier G B, *et al*. Proof-of-principle demonstration of measurement device independent quantum key distribution using polarization qubits[J]. Physical Review A, 2013, 88(5): 052303.

[17] Masanes L, Pironio S, Acín A. Secure device-independent quantum key distribution with causally independent measurement devices[J]. Nature Communications, 2010, 2(1): 238.

[18] Kang D N, He Y F. Quantum key distribution protocol based on asymmetric channels of odd coherent source[J]. Acta Optica Sinica, 2017, 37(6): 0627001.
康丹娜, 何业锋. 基于奇相干光源非对称信道的量子密钥分配协议[J]. 光学学报, 2017, 37(6): 0627001.

[19] Zhu Z D, Zhao S H, Su L H, *et al*. Research on measurement-device-independent quantum key distribution with heralded pair coherent state[J]. Laser & Optoelectronics Progress, 2017, 54(12): 122703.
朱卓丹, 赵尚弘, 苏力华, 等. 预报相干光子对的测量设备无关量子密钥分发协议研究[J]. 激光与光电子学进展, 2017, 54(12): 122703.

[20] Sun Y, Zhao S H, Dong C. Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources[J]. Acta Optica Sinica, 2016, 36(3): 0327001.
孙颖, 赵尚弘, 东晨. 基于量子存储和纠缠光源的测量设备无关量子密钥分配网络[J]. 光学学报, 2016, 36(3): 0327001.

[21] Dong C, Zhao S H, Zhao W H, *et al*. Analysis of measurement device independent quantum key distribution with an asymmetric channel transmittance efficient[J]. Acta Physica Sinica, 2014, 63(3): 030302.
东晨, 赵尚弘, 赵卫虎, 等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(3): 030302.

[22] Wu C F, Du Y N, Wang J D, *et al*. Analysis on performance optimization in measurement device independent quantum key distribution using weak coherent states[J]. Acta Physica Sinica, 2016, 65(10): 100302.
吴承峰, 杜亚男, 王金东, 等. 弱相干光源测量设备无关量子密钥分发系统的性能优化分析[J]. 物理学报, 2016, 65(10): 100302.

[23] Fasel S, Alibart O, Beveratos A, *et al*. High quality asynchronous heralded single photon source at telecom wavelength[J]. New Journal of Physics, 2004, 6(1): 628-629.

[24] Quan D X, Pei C X, Zhu C H, *et al*. New method of decoy state quantum key distribution with a heralded single-photon source[J]. Acta Physica Sinica, 2008, 57(9): 5600-5604.
权东晓, 裴昌幸, 朱畅华, 等. 一种新的预报单光子源诱骗态量子密钥分发方案[J]. 物理学报, 2008, 57(9): 5600-5604.

[25] Wang Q, Wang X B. Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources[J]. Physical Review A, 2013, 88(5): 052332.

[26] Zhu F, Wang Q. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱峰, 王琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

[27] Zhou Y Y, Zhou X J, Su B B. A measurement-device-independent quantum key distribution protocol with a heralded single photon source[J]. Optoelectronics Letters, 2016, 12(2): 148-151.